



## Kriittisen infrastruktuurin kehittyminen pitkällä aikavälillä

Juha Rautava  
Doktriiniosasto

**Yhteiskunnan toiminnoille tärkeimpiä infrastruktuureja kutsutaan kriittisiksi infrastruktuureiksi. Useat yhteiskunnan eri alat sisältävät osin kriittistä infrastruktuuria. Jotkin kriittiset osatekijät näillä aloilla eivät perinteisessä mielessä ole varsinaisesti infrastruktuuria vaan toimintoja. Ne muodostavat verkostoja tai toimintaketjuja, joita käytetään tärkeiden tuotteiden tai palvelujen jakelussa.**

Tässä lyhyessä katsauksessa keskitytään sähköenergian ja hallinnon turvallisuusverkon (TUVE) merkitykseen osana puolustusvoimille tärkeää kriittistä infrastruktuuria. Puolustusvoimien poikkeusolojen toiminnan kannalta merkittäviksi kriittisen infrastruktuurin osiksi nousevat erityisesti sähkön saatavuus ja hallinnon turvallisuusverkon (TUVE) toimivuus.

Ihmiset tarkoittavat usein eri asioita puhuessaan kriittisestä infrastruktuurista tai puhuvat samoista asioista eri käsitteillä. Ei ole myöskään vielä olemassa yleisesti toimivia analyysimalleja, joilla pystyttäisiin selvittämään monimutkaisia riippuvuusuhteita ja näiden mahdollisia vaikutuksia. Ilman näitä analyyseja lainsäädäntö, poliittinen päätöksenteko ja varsinkin resurssien allokointi kriittisen infrastruktuurin turvaamiseksi on vaikeaa. Tutkimustoiminta onkin siksi keskeisessä roolissa infrastruktuurin tarkastelussa.

### Sähkön saatavuus

Sähköntuotantokapasiteetti Suomessa ei ole tällä hetkellä riittävä vastaamaan huippukulutukseen, ja Suomi on riippuvainen sähkön tuonnista kulutushuippujen aikana. Sähkön alhainen markkinahinta on heikentänyt uusien investointien kannattavuutta, ja olemassa olevasta kapasiteetista erityisesti lauhdetuotantokapasiteettia voi poistua markkinoilta lähivuosina kannattamattomana, vaikka laitoksilla olisi vielä teknistä käyttöikää jäljellä.

Suomen nykyinen sähkön tuotantokapasiteetti koostuu pääasiassa ydinvoimasta, vesivoimasta sekä yhteistuotanto- ja lauhdevoimalaitoksista. Vesivoimakapasiteetin ei odoteta merkittävästi muuttuvan ainakaan vuoteen 2030 mennessä, sillä suurin osa potentiaalisesta lisäkapasiteetista sijaitsee suojelluissa vesistöissä. Uusien ydinvoimaloiden on oletettu tulevan käyttöön vuosina 2019 ja 2025. Tuulivoimasta on oletettu, että vuonna 2025 saavutetaan Energia- ja ilmastostrategian tavoite yhdeksän TWh:n tuulivoimatuotannosta.

Kapasiteetin ja kysynnän kehityksen tarkastelujen tuloksena voidaan todeta, että Suomen oma tuotanto ei riitä kattamaan huippukulutusta. Suomen huipunaikaisen sähköntuotantokapasiteetin on arvioitu laskevan nykytasosta vuoteen 2018 ennen Olkiluoto 3 - ydinvoimayksikön käyttöönottoa. Siihen asti huippukulutuksen ja -tuotannon ero on noin 2 800 MW normaalitalvena ja jopa 4 000 MW erittäin kylmänä talvena (keskimäärin kerran kymmenessä vuodessa). Olkiluoto 3:n (OL3) valmistuttua vaje kulutuksen ja tuotannon välillä laskee merkittävästi, mutta sähköntuotantotehon suhteen Suomi ei ole edelleenkään omavarainen. Sähkön tuonti kuitenkin riittää kattamaan eron oman tuotannon ja huippukulutuksen välillä.

Kotimaisen tuotannon tehovaje kulutukseen nähden on tarkastelelajanjaksolla suurin vuonna 2018 ennen OL3:n käyttöönottoa. Mahdollisuudet vastata huipputehon tarpeeseen siten, että lisätään Suomen omaan tuotantoa tai vähennetään kysyntää huippukulutushetkellä, ovat melko vähäiset. Tuotantokapasiteettia voitaisiin hieman lisätä kaukolämpöön liittyvässä yhteistuotannossa. Mahdollisuus lisätä tuotantoa muilla tavoilla on huippukulutushetkellä heikko.<sup>1</sup>



Kuva 1<sup>2</sup>. Kantaverkkoa Oulun seudulla.

### Turvallisuusviranomaisten yhteiset ICT-palvelut ja toimintamalli

Korkean varautumisen ja turvallisuuden vaatimukset täyttävä hallinnon turvallisuusverkko (TUVE) on valtion omistuksessa ja hallinnassa oleva viranomaisverkko, johon kuuluvat viestintäverkko, siihen liittyvät laitetilat ja laitteet sekä yhteiset tieto- ja viestintätekniset palvelut. Verkkoa käytetään viranomaisten jokapäiväisessä työssä ja se on rakennettu toimimaan luotettavasti kaikissa turvallisuustilanteissa.

TUVE-lain tultua voimaan 15.1.2015 verkko ja palvelut olivat operatiivisessa käytössä sisäministeriön ja puolustusministeriön hallinnonaloilla. TUVE-laki mahdollistaa käytön laajentamisen valtionhallinnon lisäksi kunnallisille turvallisuusviranomaisille, esimerkiksi pelastustoimen ja ensihoidon toimijoille.

Turvallisuusverkon ja yhteisten palvelujen käyttäjäkunta on tarkoitus laajentaa noin 30 000:een valtion ylimmän johdon ja ministeriöiden sekä valtion yleisen järjestyksen ja turvallisuuden, pelastustoiminnan, meripelastustoiminnan, rajaturvallisuuden,

<sup>1</sup> Pöyry Oyj: Suomen sähkötehon riittävyys ja kapasiteettirakenteen kehitys vuoteen 2030, [https://www.tem.fi/files/42026/Kapasiteetin\\_riittavyys\\_raportti\\_final.pdf](https://www.tem.fi/files/42026/Kapasiteetin_riittavyys_raportti_final.pdf), 2015

<sup>2</sup> Kuva: Sari Uusipaavalniemi



häätäkeskustoiminnan, maahanmuuton, ensihoitopalvelun ja maanpuolustuksen kannalta keskeiseen käyttäjään.

Käyttämällä TUVE-palveluja turvallisuusviranomaiset voivat toimia entistä varmemmin niin normaalioloissa kuin yhä lisääntyvässä, erityisesti tietoturvaan liittyvässä häiriötilanteissakin. Turvallisuusverkko parantaa valtiojohtoon päätöksenteon edellytyksiä, tilannekuvan muodostamista ja viranomaisten välistä tietojenvaihtoa. Yhtenäisellä TUVE-ratkaisulla poistetaan myös yksittäisten viranomaisten tarve itse rakentaa ja ylläpitää turvallisuuden ja varautumisen vaatimukset täyttäviä tietoliikenneyhteyksiä, laitetiloja ja muita tieto- ja viestintäteknisiä ratkaisuja.

Valtiovarainministeriö vastaa turvallisuusverkkotoiminnan strategisesta ja taloudellisesta ohjauksesta sekä tieto- ja viestintäteknisen varautumisen, valmiuden ja turvallisuuden ohjauksesta. Myös turvallisuusverkon palvelutuotannon ohjaus ja valvonta ovat valtiovarainministeriön vastuulla.

Ohjaustehtävää tukee valtioneuvoston asettama turvallisuusverkkotoiminnan neuvottelukunta. Neuvottelukunnassa ovat edustettuina valtioneuvoston kanslia, ulkoasiainministeriö, sisäministeriö, puolustusministeriö, liikenne- ja viestintäministeriö, sosiaali- ja terveysministeriö, puolustusvoimat, Huoltovarmuuskeskus sekä Suomen Kuntaliitto.

Turvallisuusverkon verkko- ja infrastruktuuripalveluja tuottaa valtion kokonaan omistaman Suomen Erillisverkot Oy:n tytäryhtiö Suomen Turvallisuusverkko Oy. Valtionhallinnon toimialariippumattomat ICT-palvelut tuottaa valtion tieto- ja viestintäteknikkakeskus Valtori.

poikkeusolojen tarpeita. Operaatiokeskuksen kokoonpanossa tulisi olla ratkaisuvallan omaava edustaja jokaiselta turvallisuusverkon palveluita käyttävältä hallinnonalalta. Tarvittaessa operaatiokeskuksen päätöksillä priorisoidaisiin verkon tietoliikennettä ja palveluita sekä toimijoiden omia resursseja suunnattaisiin verkon ongelmien selvittämiseen. Tämä koskee erityisesti kyberturvallisuutta. Keskuksen tehtävänä voisi olla myös sähkön saatavuuden koordinointi ja priorisointi yhdessä sähköverkon organisaatioiden kanssa.

Tällä hetkellä TUVE-verkon, kuten myös sähköverkon, palveluiden hallinta ja valvonta ovat pirstoutuneet moneen organisaatioon. Yhteisen koordinaation puuttuessa ja hallinnon ylimmän tason ollessa epäselvä, voi verkoissa ilmetä tilanteita joissa verkkojen palvelukyky vaarantuu ja tietoliikennekapasiteettia tai palveluita tulisi konfiguroida, optimoida tai priorisoida hyvinkin nopeasti, mutta sitä ei kyetä tekemään. Tämä vaarantaa myös puolustusvoimien toimintaedellytyksiä poikkeusoloissa.

### Kysely asiantuntijoille

Kriittisen infrastruktuurin pitkän aikavälin kehityssuunnista toteutettiin kysely valituille asiantuntijoille syksyllä 2015. Kysely toteutettiin sähköpostin ja internetin välityksellä sekä Puolustusvoimien tutkimuslaitoksen hallinnassa olevalla palvelimella ja Facilitate Pro -sovelluksella. Toteutus tehtiin siten, ettei yksittäisen asiantuntijan vastausta pysty erottamaan vastausaineistosta.

Asiantuntijoiksi valittiin ja kutsuttiin 45 lähinnä eri valtionhallinnon organisaatioissa ja yhteiskunnan kriittisissä yrityksissä työskentelevää ja vaikuttavaa asiantuntijaa. He edustivat seuraavia organisaatioita: puolustusministeriö, sisäministeriö, valtiovarainministeriö, puolustusvoimat, Viestintävirasto, Suomen Erillisverkot Oy, Valtori, Huoltovarmuuskeskus, Aalto-yliopisto, F-secure Oy, Atea Oy, Fingrid Oyj, Elenia Oy, Sovelto Oy ja Posti Oyj.

### Kehityksessä korostuvia kokonaisuuksia

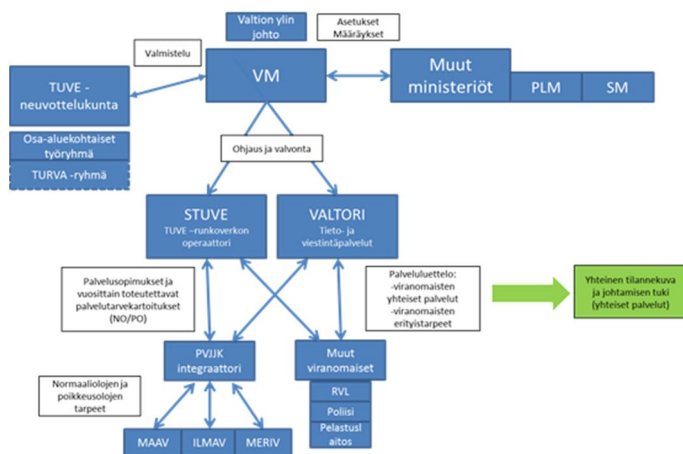
Asiantuntijakyselyssä tunnistettiin ja arvotettiin kriittiselle infrastruktuurille tärkeitä asiakokonaisuuksia. *Kokonaismaanpuolustus* ja *huoltovarmuus* nähdään merkittävänä. Kokonaismaanpuolustuksessa suomalaisen yhteiskunnan varautuminen toteutetaan kokonaisturvallisuuden periaatteella, joka tarkoittaa yhteiskunnan elintärkeiden toimintojen turvaamista viranomaisten, elinkeinoelämän sekä järjestöjen ja kansalaisten yhteistoimintana. Huoltovarmuudella tarkoitetaan kykyä sellaisten yhteiskunnan taloudellisten perustoimintojen ylläpitämiseen, jotka ovat välttämättömiä väestön elinmahdollisuuksien, yhteiskunnan toimivuuden ja turvallisuuden sekä maanpuolustuksen materiaallisten edellytysten turvaamiseksi vakavissa häiriöissä ja poikkeusoloissa.

Yhteiskunnan kriittisen infrastruktuurin turvaaminen, yhteinen tilannekuva sekä yhteinen kyky reagoida nopeisiin tilanteisiin ja johtaa kokonaismaanpuolustusta arvioidaan tärkeiksi kokonaisuuksiksi. Myös yhteiskunnan kyberturvallisuus korostuu.

Sähkön kannalta tärkeinä nähdään Suomen sähkön tuotannon omavaraisuus, sähkön tuotannossa kyky saarekkeiseen toimintaan sekä sähköverkkojen toimintavarmuus. Myös uusiutuvan energiantuotannon lisääminen koetaan tärkeäksi.

Tietotekniselle kriittiselle infrastruktuurille oleelliseksi kokonaisuuksiksi nousevat tietoliikenneverkkojen toimintavarmuus, tietojärjestelmien ja pilvipalvelujen kotimaisuus sekä tietojärjestelmien ja pilvipalvelujen kyky saarekkeiseen toimintaan (toiminta eristettynä muusta maailmasta ja vain osassa Suomea palvellen kriittisiä toimijoita).

### Turvallisuusverkkotoiminnan prosessi



Kuva 2<sup>3</sup>. Turvallisuusverkkotoiminnan prosessi.

Moni hallinnonala haluaa hallinnoida tietotekniikkaansa edelleen lähinnä omista lähtökohdistaan, jolloin resursseja käytetään tehotomasti. Tämä näkyy vielä toistaiseksi turvallisuusverkkotoiminnan prosessissa erityisesti monimutkaisuutena ja hitautena sekä ohjaavan ministeriön vähäisissä henkilöresursseissa.

### TUVE-operaatiokeskus

Tehdyn tutkimuksen ja analyysin perusteella TUVE-toiminnan koordinaation tehostamiseksi tulee edelleen tutkia TUVE-operaatiokeskuksen perustamista. Keskus voisi toimia kaikkien TUVE-verkon toimijoiden yhteisenä tilannekuva-, valvomo- ja hallintakeskuksena. Tämä tukisi erityisesti puolustusvoimien

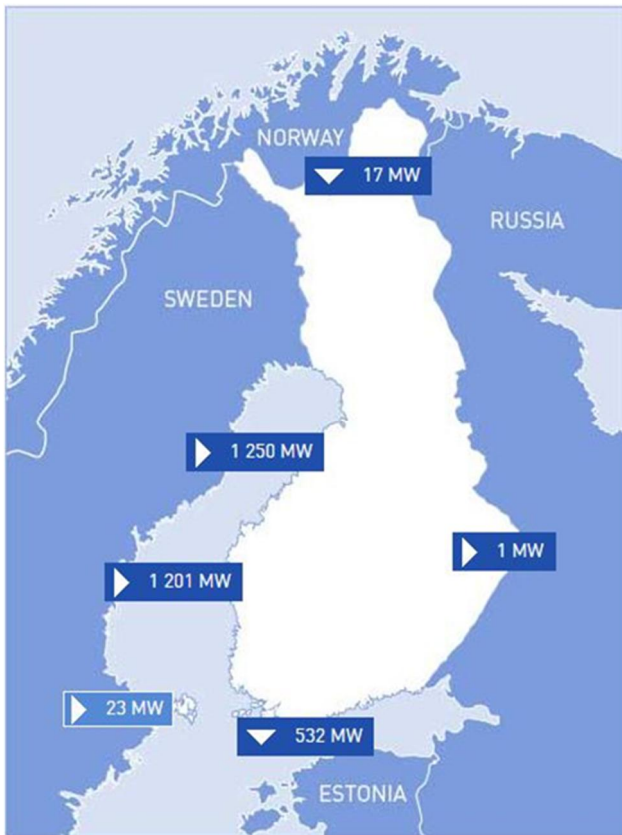
<sup>3</sup> Rautava, Juha: Kriittisen infrastruktuurin tutkimusraportti, 2015. Puolustusvoimien tutkimuslaitoksen doktriiniosaston tutkimusraportti.



### Johtopäätöksiä nykytilasta

Sähkön saatavuus ja tietotekniikan käytettävyys ovat tärkeimmät kriittisen infrastruktuurin osat. Niillä on myös suuri vaikutus muuhun kriittiseen infrastruktuuriin. Suomalainen yhteiskunta on täysin riippuvainen sähköstä ja tietotekniikasta. Puolustusjärjestelmän toimintakyky taas on täysin riippuvainen yhteiskunnan toimintakyvystä.

Suomi ei ole omavarainen sähkön tuotannon osalta ja sen saavuttaminen kestää pitkään. Suomi on tällä hetkellä täysin riippuvainen Ruotsista tuotavasta sähköstä. Sähkön tuotantokapasiteetti suhteessa kulutukseen laskee vielä vuoteen 2025 asti, jonka jälkeen suhde alkaa parantua. Sähkön jakeluverkot ovat osin päässeet rapautumaan ja sähköverkkojen toimintavarmuuden palauttaminen kestää vielä pitkään.



Kuva 3<sup>4</sup>. Voimajärjestelmän tila 10.12.2015.

Hallinnon turvallisuusverkko (TUVE) palveluineen on hyvä ratkaisu, joka takaa turvallisuusviranomaisille ja muille kriittisen infrastruktuurin toimijoille hyvät mahdollisuudet toimia vakavissa häiriötilanteissa ja poikkeusoloissa. Sen prosessi ja ohjausmalli on nykyisellään liian monimutkainen ja vaarana on, ettei se toimi vakavassa häiriötilanteessa ja poikkeusoloissa.

### Tulevaisuuden kehityssuuntia

Tulevaisuuden puolustusjärjestelmää vuoteen 2035 kehitettäessä sähkön ja tietotekniikan osalta tulee huomioida, että puolustusjärjestelmällä tulee *pahimman vaihtoehdoisen tulevaisuusennusteen* toteutuessa olla kyky toimia sellaisessa ympäristössä, jossa:

- Infrastruktuuri *ei takaa* sähkön tuotannon, sähkön jakelun ja tietotekniikan toimintavarmuutta.

- Infrastruktuuri *ei takaa* tietoliikenteen ja tietojärjestelmien käytön toimintavarmuutta.
- Julkisten tietoverkkojen *kyberturvallisuus on uhattu* ja kiistetty.
- Yhteiskunnalla *ei ole keskitettyä kykyä ennakoida ja nopeasti reagoida* kriittistä infrastruktuuria uhkaaviin tapahtumiin.
- Kokonaismaanpuolustusta ja kriittisen infrastruktuurin turvaamista *ei kyetä johtamaan* kokonaisvaltaisesti vakavassa häiriötilanteessa ja erityisesti poikkeusoloissa.
- Uusiutuva energia ja fuusioon perustuvalla ydinvoimalla tuotettu sähköenergia tulevat tuotantokäyttöön nopeammin kuin osataan ennakoida, mikä mullistaa energiamarkkinat ja talouden täydellisesti.

*Parhaassa vaihtoehdossa* tulevaisuuden puolustusjärjestelmää vuoteen 2035 kehitettäessä sähkön ja tietotekniikan osalta tulee huomioida, että puolustusjärjestelmällä tulee olla kyky toimia sellaisessa ympäristössä, jossa:

- *Infrastruktuuri takaa* sähkön tuotannon, sähkön jakelun ja tietotekniikan toimintavarmuuden.
- Suomi on sähköntuotannon osalta *omavarainen*.
- Sähkön tuotannon ja jakelun osalta kyetään saarekkeeseen toimintaan.
- *Infrastruktuuri takaa* tietoliikenteen ja tietojärjestelmien toimintavarmuuden.
- Tietoliikenteen ja tietojärjestelmien toiminnan osalta kyetään saarekkeeseen toimintaan.
- Julkisten verkkojen *kyberturvallisuus on hyvä*.
- Yhteiskunnalla *on keskitetty kyky ennakoida ja nopeasti reagoida* kriittistä infrastruktuuria uhkaaviin tapahtumiin ja toimenpiteitä harjoitellaan.
- *Hallinnon turvallisuusverkko (TUVE) takaa turvallisuusviranomaisille johtamisedellytykset kaikissa olosuhteissa* ja verkkoon on liitetty myös puolustusjärjestelmän kannalta tärkeimmät strategiset kumppanit.
- Sähkön tuotantotavoissa ja teknisissä menetelmissä tapahtuvat *muutokset osataan ennakoida ja huomioida* yhteiskuntaa ja sen osana toimivaa puolustusjärjestelmää kehitettäessä.

### Lisätietoja

*Majuri, erikoistutkija Juha Rautava palveli Puolustusvoimien tutkimuslaitoksen doktriiniosastossa strategisen analyysin tutkimuslalla ja siirtyi reserviin vuoden 2016 alussa.*

<sup>4</sup> <http://www.fingrid.fi/fi/sahkomarkkinat/voimajarjestelman-tila/Sivut/default.aspx>, 10.12.2015.